SOLUTION NOTE

SIMPLIFYING NETWORK AND SECURITY INFRASTRUCTURES FOR M&A

INTRODUCTION

Mergers and acquisitions (M&A) or even divestitures are complex processes that require careful planning and execution. One of the most challenging aspects of M&A is integrating the IT infrastructure of the two or more organizations, which is compounded by the complexity introduced by hybrid, multi-cloud environments. This process can be time-consuming, expensive and fraught with risk. However, with the right strategy and solution, organizations can simplify this process, reduce the chance of disruption, minimize the risk of exploitation by threat actors and ensure smooth and fast integration.

Many of the core challenges revolve around critical network services, including DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol) and IPAM (IP address management), commonly known as DDI. Leveraging a purpose-built platform that seamlessly integrates these components provides the foundation of an agile, secure, easily adaptable network infrastructure to keep up with emerging demands. Integrated DDI will drive unified IP address management, reducing the risk of errors, improving network stability and scalability—while maintaining a robust security posture.

UNDERSTANDING THE EXPANDING INFRASTRUCTURE

The first step to accelerating and ensuring a successful M&A starts with visibility into everything within the network, including disparate systems such as multi-cloud and hybrid environments.

Centralized IPAM (as part of an integrated DDI solution) provides organizations with detailed network inventory by gathering real-time visibility of all network assets, devices and infrastructure components (like switches, routers, etc.). This heightened visibility enables organizations to identify potential blind spots before they become major problems, allowing them to take proactive measures to ensure seamless operations during network transitions and mergers.

For example, DDI can help organizations identify configured IP networks, as well as the availability or saturation within each network IP range, giving predictive planning that is needed when integrating existing infrastructures as part of a merger or acquisition. This visibility can provide details not easily identified when evaluating the merger of multiple disparate networks—including hybrid, multi-cloud environments of both firms—giving the organizations the relevant insights needed to plan a seamless integration and identify redundancies.

AVOIDING OUTAGES AND CONFLICTS

Centralized DHCP management (as part of an integrated DDI solution), eliminates the potential for IP network collisions commonly associated with network mergers, which can significantly affect business operations—including network downtime. The financial impact varies depending on the nature of operations, but nonetheless unplanned downtime is expensive and disruptive. Overlapping IP address ranges, divergent DNS architectures and other potential conflicts typically arise when integrating multiple networks together, with any conflict resulting in network disruptions or outages. By identifying these issues early on, organizations can take steps to resolve them before they become major problems, delivering a seamless integration and ensuring business continuity.

DDI can simplify the merger of multiple networks by providing a centralized platform for managing the IP networks and addresses needed for all connected devices, users and applications—across hybrid, multi-cloud environments—with automated conflict identification and immediate resolution. An additional benefit of DDI is the ability to improve network operations by optimizing IP address utilization and reducing the number of IP addresses required while avoiding wastage or unused network ranges. This can help organizations reduce costs and improve the efficiency of their network infrastructure.

SECURING THE UNKNOWN

Cyber risk post-acquisition is a growing concern for organizations, especially with the rapidly evolving threat landscape. Sophisticated attackers purposely exploit companies when they are in flux due to their weakened operational process and general instability. Implementing DNS as a security solution is a powerful approach, helping organizations continue to secure their network and data when completing mergers and acquisition activities.

Merging another network with an existing network can pose significant security challenges:

1. **Policies and tools** used by the two networks may vary, leaving significant gaps in security posture—impacting the acquirer's corporate and compliance requirements.
2. **undetected malware** in the acquired firm's infrastructure or potential risk from the acquired firm's supply chain, due to less stringent supply chain vendor standards.
3. **Cyber attackers can exploit new vulnerabilities** from new attack surfaces that were not present on either network before the merger.
4. **Confusion and uncertainty** among employees leads to unnecessary mistakes or unidentified security gaps that can easily be exploited by attackers (e.g., attackers can set up lookalike domains for the acquired firm's internet properties, routing users and customers to those malicious domains, resulting in stolen credentials and potential credit card fraud).

To address these challenges, organizations need to take a comprehensive approach to network security, leveraging DNS as the cornerstone to their overall protection strategy. The fact that DNS is involved in all network transactions, regardless of the device type, location or destination, makes it a perfect solution to extend a common security approach to a network that is being merged. This protection can close potential gaps and protect the new networks without having to implement new security tools or make significant changes.

By taking a DNS approach to security, organizations can benefit from broad coverage that can preempt cyber threats before they become an incident. Additionally, this proactive approach reduces the burden on security teams who may be overwhelmed during the M&A process.

DIVESTITURES

In the case of divestitures, the same risks and operational hurdles exist but in reverse. Infoblox can improve this process with clear delineation of networks and assets, while ensuring that no network disruptions or downtime can occur when separating resources between two or more firms. Similarly, securing access to business-critical applications and data shouldn't be compromised during the divestiture.

Infoblox can also provide visibility post-divestiture into the company's newly modified infrastructure, enabling security teams to ensure protection and a better posture.

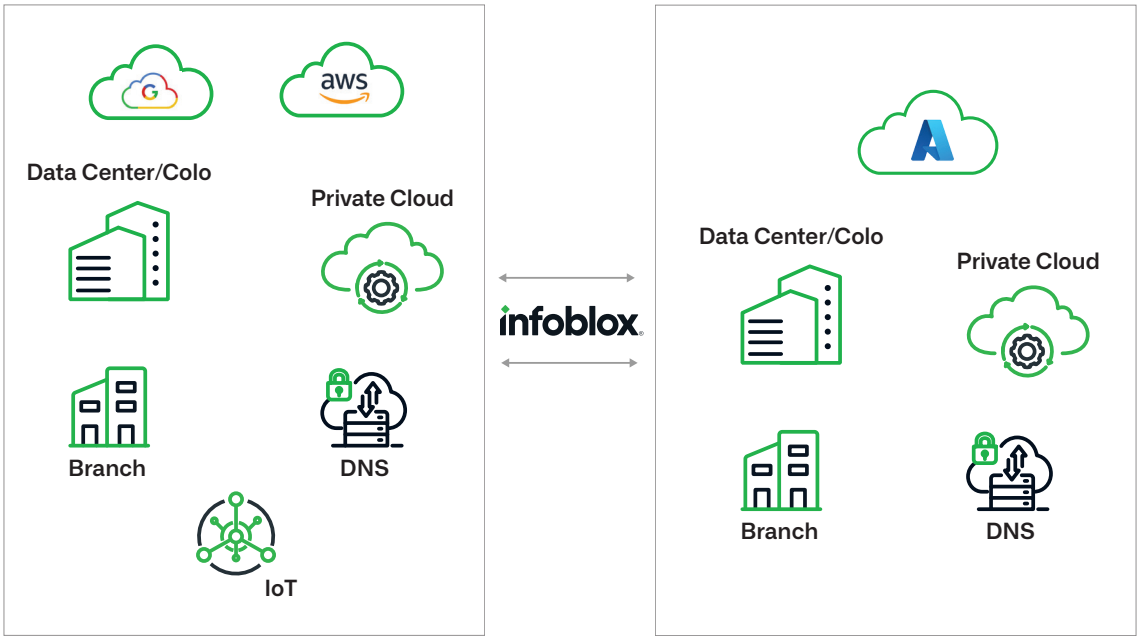

Figure 1: Infoblox helps streamline integration in an M&A

CONCLUSION

Unified DDI and DNS-based security can accelerate the mergers and acquisitions process by streamlining the integration of network infrastructure and assets, while improving the security posture of the merged entity. This approach enables the acquiring firm to realize value from the new entity faster and ensures continued business success with minimal friction.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240417v1